



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/758,889	01/16/2004	Pratik M. Mehta	016295.1518 (DC-05677)	6993
23640	7590	12/31/2007	EXAMINER	
BAKER BOTTS, LLP			YOUNG, NICOLE M	
910 LOUISIANA			ART UNIT	
HOUSTON, TX 77002-4995			PAPER NUMBER	
			2139	
			NOTIFICATION DATE	
			DELIVERY MODE	
			12/31/2007	
			ELECTRONIC	

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

debbie.allen@bakerbotts.com

Office Action Summary

Application No.

10/758,889

Applicant(s)

MEHTA ET AL.

Examiner

Nicole M. Young

Art Unit

2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 04 December 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,4-10 and 21-32 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,4-10 and 21-32 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 16 January 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/4/2007 has been entered.

This communication is in response to the amendment dated July 17, 2007. Claims 1, 4-10 and 21-32 are pending. Claims 1, 4, 6-10, 21, 25-32 are amended.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 25, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Sun et al. (US 2004/0078597)** herein referred to as Sun in further view of **Day et al. (US 7,020,476)** herein referred to as Day.

Claims 1, 25, and 30 (Currently Amended) disclose a method and system for activating a wireless network security with a wireless host, comprising:

in a wireless network having a deactivated wireless network security for the wireless network such that at least a first wireless client and a second wireless client can access the wireless without authentication, a wireless host establishing a communication connection with the first client (Fig. 4 steps 405, 410, and associated text);

in response to the communication connection, the wireless host automatically requesting from the first client a determination of whether to activate the wireless network security (Fig. 4 step 410 and associated text, where in paragraph [0044] the user is interpreted to have deactivated network security until it logged onto the new network);

the wireless host receiving from the first client a determination to activate the wireless network security (paragraph [0044] the user clicks connect to begin connecting);

in association with the determination to activate the wireless security network, the wireless host receiving an identifier code from the first client; (Fig. 4 steps 415, 425, 420 and associated text)

the wireless host determining that the received identifier code from the first client matches a unique key-code maintained by the wireless host; and (Fig. 4 steps 430-455 and associated text)

as a result of determining that the received identifier code from the first client matches the unique key-code maintained by the wireless host, the wireless host activating the deactivated wireless security network(Fig. 4 steps 430-455 and associated text)

Sun does not teach for the wireless network such that the second client cannot access the wireless network without authentication.

Day teaches for the wireless network such that the second client cannot access the wireless network without authentication (Day column 1 lines 46-59 rouge access points are disabled from secured networks).

It would be obvious to one of ordinary skill in the art at the time the invention was made to disable or disconnect unauthorized devices once network security is enabled. When a network does not have security enabled it is not secure and any devices can access it. Once the network security is enabled all devices on the network must be authorized to meet the security level of the security policy. The devices that are unauthorized would be disconnected from the network.

Claims 4, 5, 26, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Sun et al. (US 2004/0078597)** herein referred to as Sun and **Day et al. (US 7,020,476)** herein referred to as Day and further in view of **Ayyagari et al. (US 7,120,129)** herein referred to as Ayyagari.

Claims 4, 26 and 31 (Original) disclose the method and system of Claims 1, 25, and 30, further comprising following the activation of the wireless security network, changing the unique key-code to a personal code selected by the first client.

Sun does not teach but Ayyagari teaches changing the unique key-code to a personal code selected by the client. Ayyagari column 10 lines 8-30 teach changing the default SSID (interpreted as the unique-key code) on the Ad Hoc mode (interpreted to be the access point of Sun) to a personal code. This would be obvious to a person of ordinary skill in the art at the time of invention. The motivation to combine is Ayyagari column 10 lines 21-30. Ayyagari states, "the user intending to change the default SSID for AD Hock mode may create a registry variable and instantiate it to the desired Ad Hock mode SSID value. This ensure seamless operation for the normal Windows platform user".

Claim 5 (Original) discloses the method of Claim 4, further comprising resetting the unique key-code to a factory default.

Sun does not teach but Ayyagari teaches changing the unique key-code to a personal code selected by the client. Ayyagari column 10 lines 8-30 teach changing the default SSID (interpreted as the unique-key code) on the Ad Hoc mode (interpreted to be the access point of Sun) to a personal code. This would be obvious to a person of ordinary skill in the art at the time of invention. The motivation to combine is Ayyagari column 10 lines 21-30. Ayyagari states, "the user intending to change the default SSID for AD Hock mode may create a registry variable and instantiate it to the desired Ad

Hock mode SSID value. This ensure seamless operation for the normal Windows platform user". It would also be obvious to one of ordinary skill in the art at the time of invention that the user could change the key back to the factory default.

Claims 6-10, 27-29, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Sun et al. (US 2004/0078597)** and **Day et al. (US 7,020,476)** and further in view of **Jacobs et al. (US 6,993,552)** herein referred to as Jacobs.

Claim 6, 27, and 32 (Currently Amended) disclose the method and system of Claims 1, 25, and 30, further comprising:

the wireless host receiving from the first client a determination not to activate the wireless network security (Jacobs column 8 lines 16-29 teach placing an object in a queue if the user does not immediately wish to process it); and

in response to the received determination of not to activate the wireless network security, the wireless host setting a reminder flag such that the first client is automatically reminded at a future time to activate the wireless network security.

Sun does not teach but Jacobs teaches setting a reminder flag if it is determined not to activate the wireless network security. Jacobs column 8 lines 16-29 teach placing an object in a queue if the user does not immediately wish to process it. It would be obvious to one of ordinary skill in the art at the time of invention to set a reminder to

activate the wireless security if the user did not want to process it. This motivation is shown in Jacobs column 8 lines 18-27.

Claims 7 and 28 (Currently Amended) disclose the method and system of Claim 6 and 27, wherein the reminder flag comprises a reminder time period such that the first client is automatically reminded to activate the wireless security network after the expiration of the reminder time period.

The motivation to combine is the same as in the rejection of Claim 6. Sun does not teach but Jacobs does teach setting an amount of time until the user processes the object in column 8 lines 19-26.

Claims 8 and 29 (Currently Amended) disclose the method and system of Claims 6 and 27, wherein the reminder flag comprises a reminder condition such that the first client is automatically reminded to activate the wireless security network upon a subsequent communication connection.

The motivation to combine is the same as above. Sun does not teach but Jacobs teaches in column 8 lines 19-26 setting a pre-determined time to prompt the user to process the object.

Claim 9 (Currently Amended) discloses the method of Claim 6, further comprising receiving from a client a never-reminder response such that the first client is not subsequently reminded to activate the wireless network security.

The motivation to combine is the same as above. Sun does not teach but Jacobs teaches in column 8 lines 43-49 that the user can respond "NO" and the object will be deleted from the queue and never processed:

Claim 10 (Original) discloses the method of Claim 6, further comprising registering the first client to save configuration information on the client such that the wireless host recognizes the first client on a subsequent communication connection (Sun, Fig. 4 steps 415, 425 and associated text, and rejection of claim 6).

Claims 21-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Sun et al. (US 2004/0078597)** and **Day et al. (US 7,020,476)** herein referred to as Sun, as applied to claim 1 above, and further in view of **Ocepek et al. (US 2004/0049586)** herein referred to as Ocepek.

Claims 21, 22, and 23 (New) discloses the method of Claim 1, further comprising:

the second client associated with an unauthorized user accessing the wireless network before the wireless network security for the wireless network is activated due to the first client's determination to activate the wireless network security (Sun paragraph [0044] the user clicks connect to begin connecting); and
the second client associated with the unauthorized user prevented from accessing the wireless network by the wireless network security after the wireless network security for the wireless network is activated due to the client's determination to activate the

wireless network security(Sun paragraph [0044] the user clicks connect to begin connecting).

Sun teaches a client determining to activate wireless security in paragraph [0044]. Sun does not teach but Ocepek teaches a second client associated with an unauthorized user accessing the wireless network before network security is activated, Ocepek paragraphs 34-37. Ocepek teaches the unauthorized client accessing a wireless network without network security. When the client wishes to enter authorized servers the client is detected, as in paragraphs [0036]-[0037], and if authorized it is allowed to enter. If the client does not pass authorization it is prevented to access the protected server. It would be obvious to one of ordinary skill in the art at the time of invention to allow an unauthorized client to access an unauthorized wireless network and authenticate to the server if the client wishes to access authorized network services. The motivation to combine would be in paragraph [0036] of Ocepek, which states that Ocepek's system "does not add substantial overhead".

Claim 24 (New) discloses the method of Claim 1, wherein the unique key-code is a local area network (LAN) media access control (MAC) address supplied with the wireless host (Ocepek paragraph [0039]).

Response to Arguments

The Applicant argues that Sun does not teach "activating a deactivated wireless network security". The Examiner respectfully disagrees. Fig. 4 step 410 and associated text, wherein paragraph [0044] the user is interpreted to have deactivated network security until it logged onto the new network. The security is not activated, therefore it is interpreted by the Examiner to be deactivated. Authenticating through log on is interpreted to be activating the wireless security.

The Applicant argues that Sun does not teach for the wireless network such that the second client cannot access the wireless network without authentication. This argument is moot as new prior art Day et al. is used to reject the added limitation. When a network does not have security enabled it is not secure and any devices can access it. Once the network security is enabled all devices on the network must be authorized to meet the security level of the security policy. The devices that are unauthorized would be disconnected from the network.

The Examiner cites the same reasoning in maintaining the rejections of the dependent claims.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Application/Control Number:
10/758,889
Art Unit: 2139


Page 11

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nicole M. Young whose telephone number is 571-270-1382. The examiner can normally be reached on Monday through Friday, alt Fri off, 8:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NMY
12/23/2007


SYED A. ZIA
PRIMARY EXAMINER 12/21/2007